



[Faint handwritten notes at bottom]

Clean version of the Claims

Clean version of the claims with all of the changes to be made vis-à-vis the U.S. Patent 5,848,159, as follows:

1. (Twice Amended) A method for communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption, comprising the steps of:
developing k distinct random prime numbers p_1, p_2, \dots, p_k , where k is an integer greater than 2;
providing a number e relatively prime to $(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)$;
providing a composite number n equaling the product $p_1 \cdot p_2 \cdot \dots \cdot p_k$;
receiving a ciphertext word signal C which is formed by encoding a plaintext message word

signal M to a ciphertext word signal C , where M corresponds to a number representative of the message and

$$0 \leq M \leq n-1,$$

where C is a number representative of an encoded form of the plaintext message word signal M such that

$C \equiv M^e \pmod{n}$, and where e is associated with an intended recipient of the ciphertext word signal C ; and

deciphering the received ciphertext word signal C at the intended recipient having available to it the k distinct random prime numbers p_1, p_2, \dots, p_k .

2. (Twice Amended) The method according to claim 1, wherein the deciphering step includes establishing a number, d , as a multiplicative inverse of

$$e \pmod{\text{lcm}((p_1 - 1), (p_2 - 1), \dots, (p_k - 1))}, \text{ and}$$

decoding the ciphertext word signal C to the plaintext message word signal M where $M \equiv C^d \pmod{n}$.

3. (Twice Amended) A method for communications of a message signal M_i cryptographically processed with RSA public key encryption in a system having j terminals, each terminal being characterized by an encoding key $E_i = (e_i, n_i)$ and a decoding key $D_i = (d_i, n_i)$, where $i=1, 2, \dots, j$,

and the message signal M_i corresponds to a number representative of a message-to-be-received from the i^{th} terminal, the method comprising the steps of:

establishing n_i where n_i is a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\text{lcm}(p_{i,1} - 1, p_{i,2} - 1, \dots, p_{i,k} - 1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i \pmod{\text{lcm}((p_{i,1} - 1), (p_{i,2} - 1), \dots, (p_{i,k} - 1))};$$

receiving by a recipient terminal ($i = y$) from a sender terminal ($i = x, x \neq y$) a ciphertext signal C_x formed by encoding a digital message word signal M_x , wherein the encoding includes

transforming said message word signal M_x to one or more message block word signals M_x'' , each block word signal M_x'' corresponding to a number representative of a portion of said message word signal M_x in the range $0 \leq M_x'' \leq n_y - 1$, and

transforming each of said message block word signals M_x'' to a ciphertext word signal C_x that corresponds to a number representative of an encoded form of said message block word signal M_x'' where

$$C_x \equiv M_x''^{e_y} \pmod{n_y}; \text{ and}$$

deciphering the received ciphertext word signal C_x at the recipient terminal having available to it the k distinct random prime numbers $p_{y,1}, p_{y,2}, \dots, p_{y,k}$ for establishing its d_y .

4. (Twice Amended) A system for communications of a message cryptographically processed with an RSA public key encryption, comprising:

a communication channel for transmitting a ciphertext word signal C ;

encoding means coupled to said channel and adapted for transforming a transmit message word signal M to the ciphertext word signal C using a composite number, n , where n is a product of the form

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

k is an integer greater than 2, and

p_1, p_2, \dots, p_k are distinct random prime numbers,

where the transmit message word signal M corresponds to a number representative of the message and

$$0 \leq M \leq n-1$$

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$$C \equiv M^e \pmod{n}, \text{ and}$$

where e is a number relatively prime to $\text{lcm}(p_1 - 1, p_2 - 1, \dots, p_k - 1)$; and

decoding means coupled to said channel and adapted for receiving the ciphertext word signal C

from said channel and, having available to it the k distinct random prime numbers $p_1, p_2,$

\dots, p_k , for transforming the ciphertext word signal C to a receive message word signal M'

where M' corresponds to a number representative of a decoded form of the ciphertext word signal C through a relationship of the form

$$M' \equiv C^d \pmod{n}$$

where d is selected from the group consisting of a class of numbers equivalent to a multiplicative inverse of

$$e \pmod{(\text{lcm}((p_1 - 1), (p_2 - 1), \dots, (p_k - 1)))}.$$

5. (Twice Amended) A system for communications of a message cryptographically processed with an RSA public key encryption, the system having a plurality of terminals coupled by a communications channel, comprising:

a first terminal of the plurality of terminals characterized by an encoding key

$$E_A = (e_A, n_A) \text{ and a decoding key } D_A = (d_A, n_A),$$

where n_A is a composite number of the form

$$n_A = p_{A,1} \cdot p_{A,2} \cdot \dots \cdot p_{A,k}$$

where

k is an integer greater than 2,

$p_{A,1}, p_{A,2}, \dots, p_{A,k}$ are distinct random prime numbers,

e_A is relatively prime to

$$\text{lcm}(p_{A,1} - 1, p_{A,2} - 1, \dots, p_{A,k} - 1), \text{ and}$$

d_A is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_A \pmod{\text{lcm}((p_{A,1} - 1), (p_{A,2} - 1), \dots, (p_{A,k} - 1))}$; and

a second terminal of the plurality of terminals having

blocking means for transforming a first message, which is to be transmitted on said communications channel from said second terminal to said first terminal, into one or more transmit message word signals M_B , where each M_B corresponds to a number representative of said first message in the range

$$0 \leq M_B \leq n_A - 1,$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that corresponds to a number representative of an encoded form of said first message through a relationship of the form

$$C_B \equiv M_B^{e_A} \pmod{n_A},$$

said first terminal having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_B from said channel and, having available to it the k distinct random prime numbers $p_{A,1}, p_{A,2}, \dots, p_{A,k}$, for transforming each of said ciphertext word signals C_B to a receive message word signal M'_B , and

means for transforming said receive message word signal M'_B to said first message, where M'_B corresponds to a number representative of a decoded form of C_B through a relationship of the form

$$M'_B \equiv C_B^{d_A} \pmod{n_A}.$$

6. (Twice Amended) The system according to claim 5 wherein said second terminal is characterized by an encoding key $E_B = (e_B, n_B)$ and a decoding key $D_B = (d_B, n_B)$, where n_B is a composite number of the form

$$n_B = p_{B,1} p_{B,2} \dots p_{B,k}$$

where k is an integer greater than 2,

$p_{B,1}, p_{B,2}, \dots, p_{B,k}$ are distinct random prime numbers,

e_B is relatively prime to

$\text{lcm}(p_{B,1}-1, p_{B,2}-1, \dots, p_{B,k}-1)$, and

d_B is selected from the group consisting of a class of numbers equivalent to a multiplicative inverse of

$e_B \pmod{\text{lcm}((p_{B,1}-1), (p_{B,2}-1), \dots, (p_{B,k}-1))}$,

said first terminal further having

blocking means for transforming a second message, [-to-be-transmitted] which is to be transmitted on said communications channel from said first terminal to said second terminal, to one or more transmit message word signals M_A , where each M_A corresponds to a number representative of said message in the range

$$0 \leq M_A \leq n_B - 1$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, where C_A corresponds to a number representative of an encoded form of said second message through a relationship of the form

$$C_A \equiv M_A^{e_B} \pmod{n_B}$$

said second terminal further having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_A from said channel and, having available to it the k distinct random prime numbers $p_{B,1}, p_{B,2}, \dots, p_{B,k}$, for transforming each of said ciphertext word signals to a receive message word signal M'_A , and means for transforming said receive message word signals M'_A to said second message, where M'_A corresponds to a number representative of a decoded form of C_A through a relationship of the form

$$M'_A \equiv C_A^{d_B} \pmod{n_B}.$$

7. (Amended) A method for communications of a message cryptographically processed with an RSA public key encryption, comprising the steps of:

developing k factors of a composite number n , the k factors being distinct random prime numbers and k is an integer larger than two ($k > 2$);

providing a number e relatively prime to a lowest common multiplier of the k factors;

providing the composite number n ;

receiving a ciphertext word signal C which is formed by encoding a digital message word signal M to the ciphertext word signal C, where said digital message word signal M corresponds to a number representative of said message and

$$0 \leq M \leq n-1,$$

where said ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \dots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}, \dots, a_0 are numbers; and

deciphering the received ciphertext word signal C at an intended recipient with knowledge of the k factors.

8. Cancelled.

9. (Twice Amended) A system for communications of message signals cryptographically processed with RSA public key encryption, comprising:

j terminals including first and second terminals, each of the j terminals being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where $i=1, 2, \dots, j$, each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is transmitted from an i^{th} terminal, and

$$0 \leq M_i \leq n_i - 1,$$

n_i being a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to

$$\text{lcm}(p_{i,1}-1, p_{i,2}-1, \dots, p_{i,k}-1), \text{ and}$$

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i \pmod{(\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \dots, (p_{i,k}-1)))};$$

said first terminal including

means for encoding a digital message word signal M_1 to be transmitted from said first terminal ($i=1$) to said second terminal ($i=2$), said encoding means transforming said digital message word signal M_1 to a signed message word signal M_{1s} using a relationship of the form

$$M_{1s} \equiv M_1^{d_1} \pmod{n_1}; \text{ and}$$

means for transmitting said signed message word signal M_{1s} from said first terminal to said second terminal, wherein said second terminal includes

means for decoding said signed message word signal M_{1s} to said digital message word signal M_1 .

10. (Twice Amended) The system of claim 9, wherein the means for decoding said signed message word signal M_{As} includes means for transforming said signed message word signal M_{As} using a relationship of the form

$$M_1 \equiv M_{1s}^{e_1} \pmod{n_1}.$$

11. (Twice Amended) A communications system for transferring a message signal cryptographically processed with RSA public key encryption, the communications system comprising:

j communication stations including first and second stations, each of the j communication stations being characterized by an encoding key $E_i=(e_i, n_i)$ and a decoding key $D_i=(d_i, n_i)$, where $i=1, 2, \dots, j$, each of the j communication stations being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is received from an i^{th} communication station, and

$$0 \leq M_i \leq n_i - 1$$

n_i being a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\text{lcm}(p_{i,1} - 1, p_{i,2} - 1, \dots, p_{i,k} - 1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a
multiplicative inverse of

$$e_i \pmod{\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \dots, (p_{i,k}-1))},$$

said first station including

means for encoding a digital message word signal M_1 to be transmitted from said
first station ($i=1$) to said second station ($i=2$),

means for transforming said digital message word signal $[M_A] M_1$ to one or more
message block word signals $[M_A'] M_1''$, each block word signal $[M_A'] M_1''$
being a number representative of a portion of said message word signal M_1
in the range

$$0 \leq M_1'' \leq n_2 - 1, \text{ and}$$

means for transforming each of said message block word signals M_1'' to a
ciphertext word signal C_1 using a relationship of the form

$$C_1 \equiv M_1''^{e_2} \pmod{n_2}; \text{ and}$$

means for transmitting said ciphertext word signals C_1 from said first station to said second
station, wherein said second station includes

means for deciphering said ciphertext word signals C_1 using $p_{2,1}, p_{2,2}, \dots, p_{2,k}$ to
produce said message word signal M_1 .

12. (Twice Amended) The communications system of claim 11, wherein the deciphering means
includes

means for decoding said ciphertext word signals C_1 to said message block word
signals M_1'' using a relationship of the form

$$M_1'' \equiv C_1^{d_2} \pmod{n_2}, \text{ and}$$

means for transforming said message block word signals M_1'' to said message
word signal M_1 .

13. (Twice Amended) A system for communications of a message cryptographically processed
with RSA public key encryption, comprising:

a first station; and

a second station communicatively connected to the first station,

the first station having

encoding means for transforming a transmit message word signal M to a ciphertext word signal C where the transmit message word signal M corresponds to a number representative of a message and

$$0 \leq M \leq n-1$$

n being a composite number formed as a product of at least 3 factors, the at least 3 factors being distinct random prime numbers, and

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \dots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}, \dots, a_0 are numbers; and

means for transmitting the ciphertext word signal C to the second station, wherein the second station includes means for deciphering the ciphertext word signal C using the at least 3 factors to produce the message.

New Claims:

14. (Amended) A method of communicating a message cryptographically processed with an RSA public key encryption, comprising the steps of:

selecting a public key portion e associated with a recipient intended for receiving the message;

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

computing a composite number, n , as a product of the k distinct random prime numbers;

receiving a ciphertext message formed by encoding a plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, where M represents the

message, where $0 \leq M \leq n-1$ and where the sender knows n and the public key portion e but has no access to the k distinct random prime numbers, p_1, p_2, \dots, p_k ; and
deciphering at the recipient the received ciphertext message data C to produce the message, the recipient having access to the k distinct random prime numbers, p_1, p_2, \dots, p_k .

15. (Amended) The method according to claim 14, comprising the further step of:
establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1}(\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))),$$

wherein the deciphering step includes decoding the ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d (\text{mod } n)$.

16. (Amended) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e ;

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1}(\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)));$$

computing a composite number, n , as a product of the k distinct random prime numbers;

receiving a ciphertext message data C representing an encoded form of a plaintext message data M ; and

decoding the received ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d (\text{mod } n)$, the decoding performed by a recipient owning the private key portion d and having access to the k distinct random prime numbers, p_1, p_2, \dots, p_k .

17. (Amended) The method according to claim 16, wherein the ciphertext message data C is formed by encoding the plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, wherein $0 \leq M \leq n-1$ and wherein n and the public key portion e are accessible to the sender although it has no access to the k distinct random prime numbers, p_1, p_2, \dots, p_k .

18. (Amended) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e ;

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

establishing a private key portion d by a relationship to the public key portion e of the form

$$d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))};$$

computing a composite number, n , as a product of the k distinct random prime numbers;

encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$

receiving the signed message M_s ; and

deciphering the signed message to produce the plaintext message data M .

19. (Amended) The method of claim 18, wherein the deciphering step includes:

decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

20. (Amended) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

sending to a recipient a cryptographically processed message formed by

assigning a number M to represent the message in plaintext message form, and

cryptographically transforming the assigned number M from the plaintext message form

to a number C that represents the message in an encoded form, wherein the number C is a function of

the assigned number M ,

a number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e having been obtained by the sender are associated with the recipient to which the message is intended; and

receiving the cryptographically processed message which is decipherable by the recipient based on

the number n ,

another exponent d , and

the number C ,

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers.

21. (Amended) The method according to claim 20,

wherein the cryptographically transforming step includes using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent d is established based on the at least three distinct random prime numbers,

p_1, p_2, \dots, p_k using a relationship of the form $d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))}$,

and

wherein the cryptographically processed message is deciphered using a relationship of the form
$$M \equiv C^d \pmod{n}.$$

22. (Amended) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

receiving from a sender a cryptographically processed message, in the form of a number C , which is decipherable by the recipient based on a number n , an exponent d , and the number C ; and

deciphering the cryptographically processed message,

wherein a number M represents a plaintext form of the message, wherein the number C represents a cryptographically encoded form of the message and is a function of the number M ,

the number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e are associated with the recipient to which the message is intended, and

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers.

23. (Amended) The method according to claim 22,

wherein the number C is formed using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent d is established based on the at least three distinct random prime numbers,

p_1, p_2, \dots, p_k using a relationship of the form $d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))}$,

and wherein the number M is obtained using a relationship of the form $M \equiv C^d \pmod{n}$.

24. (Amended) The method according to claim 21,

wherein p and q are a pair of prime numbers the product of which equals n ,
wherein the deciphering the number C to derive the number M is divided into subtasks, one
subtask for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q ,
whereby for a given length of n it takes fewer computational cycles to perform the deciphering
relative to the number of computational cycles for performing such deciphering if the pair
of prime numbers p and q were used instead.

25. (Amended) The method according to claim 22,

wherein p and q are a pair of prime numbers the product of which equals n ,
wherein the deciphering the number C to derive the number M is divided into subtasks, one
subtask for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q ,
whereby for a given length of n it takes fewer computational cycles to perform the deciphering
relative to the number of computational cycles for performing such deciphering if the pair of
prime numbers p and q were used instead.

26. (Amended) The method according to claim 20,

wherein p and q are a pair of prime numbers the product of which equals n , and
wherein developing the at least three distinct random prime numbers and computing n is
performed, including for n that is more than 600 digits long, in less time than it takes to develop
the pair of prime numbers p and q and compute that n .

27. (Amended) The method according to claim 22,

wherein p and q are a pair of prime numbers the product of which equals n , and
wherein developing the at least three distinct random prime numbers and computing n is
performed, including for n that is more than 600 digits long, in less time than it takes to develop
the pair of prime numbers p and q and compute that n .

28. (Amended) The method according to claim 14,

wherein p and q are a pair of prime numbers the product of which equals n ,

wherein the deciphering step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q ,

whereby for a given length of n it takes fewer computational cycles to perform the deciphering step relative to the number of computational cycles for performing such deciphering step if the pair of prime numbers p and q were used instead.

29. (Amended) The method according to claim 14,

wherein p and q are a pair of prime numbers the product of which equals n , and

wherein developing the k distinct random prime numbers and computing the composite number n are performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n .

30. (Amended) The method according to claim 16,

wherein p and q are a pair of prime numbers the product of which equals n ,

wherein the decoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q ,

whereby for a given length of n it takes fewer computational cycles to perform the decoding step relative to the number of computational cycles for performing such decoding step if the pair of prime numbers p and q were used instead.

31. (Amended) The method according to claim 16,

wherein p and q are a pair of prime numbers the product of which equals n , and

wherein developing the k distinct random prime numbers and computing the composite n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n .

32. (Amended) The method according to claim 18,

wherein p and q are a pair of prime numbers the product of which equals n ,

wherein the encoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q ,

whereby for a given length of n it takes fewer computational cycles to perform the encoding step relative to the number of computational cycles for performing such encoding step if the pair of prime numbers p and q were used instead.

33. (Amended) The method according to claim 18,

wherein p and q are a pair of prime numbers the product of which equals n , and

wherein developing the k distinct random prime numbers and computing the composite number n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n .

34. (Amended) The method according to claim 14, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q , is decipherable with multi-prime ($k > 2$) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, \dots, p_k .

35. (Amended) The method according to claim 9, wherein the signed message word signal M_{1s} , formed from the digital message word signal M_1 being cryptographically processed at the first terminal with multi-prime ($k > 2$) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, \dots, p_k , is decipherable at the second terminal with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q .

36. (Amended) The method according to claim 16, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q , is decipherable by the decoding with multi-prime ($k > 2$) RSA public key encryption characterized

by the composite number n being computed as the product of the k distinct random prime numbers, $p_1, p_2, \dots p_k$.

37. (Amended) The method according to claim 18, wherein the signed message M_s , formed from the plaintext message data M being cryptographically processed at the sender with multi-prime ($k > 2$) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, $p_1, p_2, \dots p_k$, is decipherable by the decoding at the recipient with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q .

38. (Amended) The method according to claim 20, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q , is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

39. (Amended) The method according to claim 22, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q , is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

40. (Amended) A cryptography method for local storage of data by a private key owner, comprising the steps of:

selecting a public key portion e ;

developing k distinct random prime numbers, $p_1, p_2, \dots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots p_k-1$, is relatively prime to the public key portion e ;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1} (\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))) ;$$

computing a composite number, n , as a product of the k distinct random prime numbers that are factors of n , where only the private key owner knows the factors of n ; and
 encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form $C \equiv M^e (\text{mod } n)$, where $0 \leq M \leq n-1$, whereby the ciphertext data C is decipherable only by the private key owner having available to it the factors of n .

41. The cryptography method in accordance with claim 40, further comprising the step of:
 decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d (\text{mod } n)$.

42. (Amended) A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to communicate with the plurality of stations via the communications medium sending a receiving messages cryptographically processed with an RSA public key encryption, the host system including

at least one cryptosystem configured for

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to a public key portion e that is associated with the host system,

computing a composite number, n , as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e

in the form of $d \equiv e^{-1} (\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$,

in response to an encoding request from the host system, encoding a plaintext message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form $C \equiv M^e (\text{mod } n)$, where $0 \leq M \leq n-1$,

in response to a decoding request from the host system, decoding a ciphertext message data C' communicated via the host producing therefrom a plaintext message data M' using a relationship of the form $M' \equiv C'^d \pmod{n}$).

43. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem communicatively coupled to and receiving from the bus encoding and decoding requests, the cryptosystem being configured for providing a public key portion e ,

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ,

computing a composite number, n , as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} \pmod{((p_1-1) \cdot (p_2-1) \cdots (p_k-1))}$,

in response to an encoding request from the bus, encoding a plaintext form of a first message M to produce C , a ciphertext form of the first message, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$, and

in response to an decoding request from the host system, decoding C' , a ciphertext form of a second message, to produce M' , a plaintext form of the second message, using a relationship of the form $M' \equiv C'^d \pmod{n}$, the first and second messages being distinct or one and the same.

44. The system of claim 42, wherein the at least one cryptosystem includes a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

45. (Amended) The system of claim 42, wherein the at least one cryptosystem includes a processor,
a data-address bus,

a memory coupled to the processor via the data-address bus,

a data encryption standard (DES) unit coupled the memory and the processor via the data-address bus,

a plurality of exponentiator elements coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. (Amended) The system of claim 45, wherein the memory and each of the plurality of exponentiator elements has its own DES unit that cryptographically processes message data received/returned from/to the processor.

47. (Amended) The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor, including secure, insecure and exponentiator elements address spaces, and wherein the DES unit is configured to recognize the secure and exponentiator elements address spaces and to automatically encode message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when the processor is accessing the insecure memory address spaces, the DES unit being further configured to decode encoded message data received from the memory before it is provided to the processor.

48. The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

49. The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors p_1, p_2, \dots, p_k .

50. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding request providing a plaintext message M to be encoded,

obtaining a public key that includes an exponent e and a modulus n , a representation of the modulus n existing in the memory in the form of its k distinct random prime number factors p_1, p_2, \dots, p_k , where $k \geq 3$,

constructing subtasks, one subtask for each of the k factors, to be executed by the exponentiator elements for producing respective ones of the subtask values, C_1, C_2, \dots, C_k , and

forming a ciphertext message C from the subtask values C_1, C_2, \dots, C_k ,

wherein the ciphertext message C is decipherable using a private key that includes the modulus n and an exponent d which is a function of e .

51. (Amended) The system of claim 50 wherein each one of the subtasks C_1, C_2, \dots, C_k is developed using a relationship of the form $C_i \equiv M_i^{e_i} \pmod{p_i}$, where $M_i \equiv M \pmod{p_i}$, and $e_i \equiv e \pmod{p_i - 1}$, and where $i=1, 2, \dots, k$.

52. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding/decoding request provided with a plaintext/ciphertext message M/C to be encoded/decoded and with or without a public/private key that includes an exponent e/d and a modulus n a representation of which exists in the memory in the form of its k distinct random prime number factors p_1, p_2, \dots, p_k , where $k \geq 3$,

obtaining the public/private key from the memory if the encoding/decoding request is provided without the public/private key,
constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $M_1, M_2, \dots M_k, C_1, C_2, \dots C_k$, and forming the ciphertext/plaintext message C/M from the subtask values $C_1, C_2, \dots C_k/M_1, M_2, \dots M_k$.

53. (Amended) The system of claim 52 wherein when produced each one of the subtasks $C_1, C_2, \dots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} \pmod{p_i}$, where $C_i \equiv C \pmod{p_i}$, and $e_i \equiv e \pmod{p_i - 1}$, and where $i=1, 2, \dots k$.

54. (Amended) The system of claim 52 wherein when produced each one of the subtasks $M_1, M_2, \dots M_k$ is developed using a relationship of the form $M_i \equiv C_i^{d_i} \pmod{p_i}$, where $M_i \equiv M \pmod{p_i}$, and $d_i \equiv d \pmod{p_i - 1}$, and where $i=1, 2, \dots k$.

55. The system of claim 54, wherein the private key exponent d relates to the public key exponent e via $d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))}$.

56. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e ;

means for developing k distinct random prime numbers, $p_1, p_2, \dots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots p_k-1$, is relatively prime to the public key portion e ;

means for establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))}$;

means for computing a composite number, n , as a product of the k distinct random prime numbers;

means for receiving a ciphertext message data C ; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

57. The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C , using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

58. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e ;

means for developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

means for establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1} \pmod{(p_1-1) \cdot (p_2-1) \cdots (p_k-1)}$;

means for computing a composite number, n , as a product of the k distinct random prime numbers; and

means for encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$, the signed message M_s being decipherable using the public key portion e .

59. (Amended) The system of claim 58 further comprising the step of:

means for decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

60. (Amended) The system of claim 57, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

61. (Amended) The system of claim 59, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

Reissue 09/694,416
Collins et al.

THE
FEDERAL
BUREAU
OF
INVESTIGATION
OF
THE
DEPARTMENT
OF
JUSTICE
WASHINGTON, D. C.

File Compare Results to Show Changes to the Claims Since the Preliminary Amendment

Clean version of the Claims

Clean version of the claims with all of the changes to be made vis-à-vis the U.S. Patent 5,848,159, as follows:

1. (Twice Amended) A method of ~~processing a message for use in cryptographic communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption, comprising the steps of:~~
developing k distinct random prime numbers p_1, p_2, \dots, p_k , where k is an integer greater than 2;
providing a number e relatively prime to $(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)$;
providing a composite number, n , as a equaling the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ where k is an integer greater than 2, and p_1, p_2, \dots, p_k are distinct random prime numbers; and;
receiving a ciphertext word signal C which is formed by encoding a plaintext message word signal M to a ciphertext word signal C , where M corresponds to a number representative of the message and
 $0 \leq M \leq n-1$,
where C is a number representative of an encoded form of the plaintext message word signal M such that
 $C \equiv M^e \pmod{n}$, and where e is associated with an intended recipient of the ciphertext word signal C ; and
where e is a number relatively prime to $(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)$.
deciphering the received ciphertext word signal C at the intended recipient having available to it the k distinct random prime numbers p_1, p_2, \dots, p_k .

2. (Twice Amended) The method according to claim 1, ~~comprising~~wherein the ~~further deciphering step of:~~includes

establishing a number, d , as a multiplicative inverse of
 $e(\text{mod}(\text{lcm}((p_1 - 1), (p_2 - 1), \dots, (p_k - 1))))$; and

decoding the ciphertext word signal C to the plaintext message word signal M where
 $M \equiv C^d \pmod{n}$.

3. (Twice Amended) A method for communications of processing a message signal M_i for
usecryptographically processed with RSA public key encryption in a communications system
 having j terminals, each terminal being characterized by an encoding key $E_i = (e_i, n_i)$ and a
 decoding key $D_i = (d_i, n_i)$, where $i=1, 2, \dots, j$, and the message signal M_i
~~corresponding~~ corresponds to a number representative of a message-to-be-transmitted received
 from the i^{th} terminal, the method comprising the steps of:
~~computing~~ establishing n_i where n_i is a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\text{lcm}(p_{i,1} - 1, p_{i,2} - 1, \dots, p_{i,k} - 1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a
 multiplicative inverse of

$$e_i \pmod{(\text{lcm}((p_{i,1} - 1), (p_{i,2} - 1), \dots, (p_{i,k} - 1)))};$$

receiving by a recipient terminal ($i = y$) from a sender terminal ($i = x, x \neq y$) a ciphertext
signal C_x formed by encoding a digital message word signal M_1 for transmission from a
first terminal ($i=1$) to a second terminal ($i=2$) M_x , said encoding step including wherein the
sub-step of: encoding includes

transforming said message word signal M_1 M_x to one or more message block word signals
 M_1 M_x ", each block word signal M_1 M_x " corresponding to a number representative
 of a portion of said message word signal M_1 M_x in the range $0 \leq M_1$ M_x " $\leq n_2 - 1, n_y -$
1, and

transforming each of said message block word signals M_1 M_x " to a ciphertext word signal
 C_1 C_x that corresponds to a number representative of an encoded form of said
 message block word signal M_1 M_x " where

$$C_x \equiv M_x^{e_y} \pmod{n_y}; \text{ and}$$

deciphering the received ciphertext word signal C_x at the recipient terminal having available to it the k distinct random prime numbers $p_{y,1}, p_{y,2}, \dots, p_{y,k}$ for establishing its d_y .

4. (Twice Amended) A cryptographiesystem for communications systemof a message cryptographically processed with an RSA public key encryption, comprising:

a communication channel adapted for transmitting a ciphertext word signal C ~~that relates to a transmit message word signal M ;~~

encoding means coupled to said channel and adapted for transforming ~~thea~~ transmit message word signal M to the ciphertext word signal C using a composite number, n , where n is a product of the form

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

k is an integer greater than 2, and

p_1, p_2, \dots, p_k are distinct random prime numbers,

where the transmit message word signal M corresponds to a number representative of athe message and

$$0 \leq M \leq n-1$$

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form~~[and corresponds to]~~

$$C \equiv M^e \pmod{n}, \text{ and}$$

where e is a number relatively prime to $\text{lcm}(p_1 - 1, p_2 - 1, \dots, p_k - 1)$; and

decoding means coupled to said channel and adapted for receiving the ciphertext word signal C

from said channel and, having available to it the k distinct random prime numbers $p_1, p_2,$

$\dots, p_k,$ for transforming the ciphertext word signal C to a receive message word signal M'

where M' corresponds to a number representative of a decoded form of the ciphertext word signal C through a relationship of the form

$$M' \equiv C^d \pmod{n}$$

where d is selected from the group consisting of a class of numbers equivalent to a multiplicative inverse of

$$e(\text{mod}(\text{lcm}((p_1 - 1), (p_2 - 1), \dots, (p_k - 1)))).$$

5. (Twice Amended) A cryptographiesystem for communications of a message cryptographically processed with an RSA public key encryption, the system having a plurality of terminals coupled by a communications channel, comprising:

a first terminal of the plurality of terminals characterized by an encoding key

$$E_A = (e_A, n_A) \text{ and a decoding key } D_A = (d_A, n_A),$$

where n_A is a composite number of the form

$$n_A = p_{A,1} \cdot p_{A,2} \cdot \dots \cdot p_{A,k}$$

where

k is an integer greater than 2,

$p_{A,1}, p_{A,2}, \dots, p_{A,k}$ are distinct random prime numbers,

e_A is relatively prime to

$$\text{lcm}(p_{A,1} - 1, p_{A,2} - 1, \dots, p_{A,k} - 1), \text{ and}$$

d_A is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_A (\text{mod}(\text{lcm}((p_{A,1} - 1), (p_{A,2} - 1), \dots, (p_{A,k} - 1)))); \text{ and}$$

a second terminal of the plurality of terminals having

blocking means for transforming a first message, which is to be transmitted on said communications channel from said second terminal to said first terminal, ~~to~~into one or more transmit message word signals M_B , where each M_B corresponds to a number representative of said first message in the range

$$0 \leq M_B \leq n_A - 1,$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that corresponds to a number representative of an encoded form of said first message ~~through~~through a relationship of the form

$$C_B \equiv M_B^{e_A} (\text{mod } n_A),$$

said first terminal having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_B from said channel and, having available to it the k distinct random prime numbers $p_{A,1}, p_{A,2}, \dots, p_{A,k}$ for transforming each of said ciphertext word signals C_B to a receive message word signal M'_B , and means for transforming said receive message word signal M'_B to said first message, where M'_B corresponds to a number representative of a decoded form of C_B through a relationship of the form

$$M'_B \equiv C_B^{d_A} \pmod{n_A}.$$

6. (Twice Amended) The system according to claim 5 wherein said second terminal is characterized by an encoding key $E_B = (e_B, n_B)$ and a decoding key $D_B = (d_B, n_B)$, where n_B is a composite number of the form

$$n_B = p_{B,1} \cdot p_{B,2} \cdot \dots \cdot p_{B,k}$$

where k is an integer greater than 2,

$p_{B,1}, p_{B,2}, \dots, p_{B,k}$ are distinct random prime numbers,

e_B is relatively prime to

$\text{lcm}(p_{B,1}-1, p_{B,2}-1, \dots, p_{B,k}-1)$, and

d_B is selected from the group consisting of a class of numbers equivalent to a multiplicative inverse of

$$e_B \pmod{(\text{lcm}((p_{B,1}-1), (p_{B,2}-1), \dots, (p_{B,k}-1)))},$$

said first terminal further having

blocking means for transforming a second message, [-to-be-transmitted] which is to be transmitted on said communications channel from said first terminal to said second terminal, to one or more transmit message word signals M_A , where each M_A corresponds to a number representative of said message in the range

$$0 \leq M_A \leq n_B - 1$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, where C_A corresponds to a number

representative of an encoded form of said second message through a relationship of the form

$$C_A \equiv M_A^{e_B} \pmod{n_B}$$

said second terminal further having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_A from said channel and, having available to it the k distinct random prime numbers $p_{B,1}, p_{B,2}, \dots, p_{B,k}$, for transforming each of said ciphertext word signals to a receive message word signal M'_A , and means for transforming said receive message word signals M'_A to said second message, where M'_A corresponds to a number representative of a decoded form of C_A through a relationship of the form

$$M'_A \equiv C_A^{d_B} \pmod{n_B}.$$

7. (Amended) A method of ~~processing a message for use in cryptographic communications of a~~ message cryptographically processed with an RSA public key encryption, comprising the steps of:

~~developing k factors of a composite number, n, as a product of at least 3 whole number factors greater than one, the k factors being distinct random prime numbers; and k is an integer larger than two ($k > 2$);~~

providing a number e relatively prime to a lowest common multiplier of the k factors;

providing the composite number n;

receiving a ciphertext word signal C which is formed by encoding a digital message word signal

M to the ciphertext word signal C, where said digital message word signal M corresponds to a number representative of a said message and

$$0 \leq M \leq n-1,$$

where said ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \dots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}, \dots, a_0 are numbers; and

deciphering the received chiphertext word signal C at an intended recipient with knowledge of the k factors.

8. (Amended) A method according to claim 7 wherein said encoding step further includes the step of

~~transforming said digital message word signal M to said ciphertext word signal C by the performance of a first ordered succession of invertible operations on M, and wherein the method further comprises the step of:~~

~~decoding said ciphertext word signal C to said digital message word signal M by the performance of a second ordered succession of invertible operations on C, where each of the invertible operations of said second ordered succession is the inverse of a corresponding one of said first ordered succession, and where the order of said invertible operations in said second ordered succession is reversed with respect to the order of corresponding invertible operations in said first ordered succession.~~

8. Cancelled.

9. (Twice Amended) A ~~communication~~ system for processing communications of message signals cryptographically processed with RSA public key encryption, comprising:

j terminals including first and second terminals, each of the j terminals being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$, where $i=1, 2, \dots, j$, each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} terminal corresponds to an i^{th} message signal M_i is transmitted from an i^{th} terminal, and

$$0 \leq M_i \leq n_i - 1,$$

n_i being a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to

$\text{lcm}(p_{i,1}-1, p_{i,2}-1, \dots, p_{i,k}-1)$, and
 d_i is selected from the group consisting of the class of numbers equivalent
to a multiplicative inverse of
 $e_i \pmod{\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \dots, (p_{i,k}-1))}$;
said first terminal including

means for encoding a digital message word signal M_1 to be transmitted
from said first terminal ($i=1$) to said second terminal ($i=2$), said encoding
means transforming said digital message word signal M_1 to a signed
message word signal M_{1s} using a relationship of the form

~~10. (Amended) The communication system of claim 9 further comprising:~~

~~$M_{1s} \equiv M_1^{d_1} \pmod{n_1}$; and~~

~~means for transmitting said signed message word signal M_{1s} from said first terminal to said
second terminal, wherein said second terminal including includes~~

~~means for decoding said signed message word signal M_{1s} to said digital message
word signal M_{1s}~~

~~10. (Twice Amended) The system of claim 9, wherein the means for decoding said signed
message word signal M_{1s} includes means for transforming said signed message word
signal M_{1s} using a relationship of the form~~

$$M_1 \equiv M_{1s}^{e_1} \pmod{n_1}.$$

11. (Twice Amended) A communications system for transferring a message signal
cryptographically processed with RSA public key encryption, the communications system
comprising:

j communication stations including first and second stations, each of the j communication
stations being characterized by an encoding key $E_i=(e_i, n_i)$ and a decoding key $D_i=(d_i,$

n_i), where $i=1, 2, \dots, j$, each of the j communication stations being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is received from an i^{th} communication station corresponds to an i^{th} message signal M_i , and

$$0 \leq M_i \leq n_i - 1$$

n_i being a composite number of the form

$$n_i = p_{i,1} \cdot p_{i,2} \cdot \dots \cdot p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \dots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\text{lcm}(p_{i,1} - 1, p_{i,2} - 1, \dots, p_{i,k} - 1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i \pmod{\text{lcm}((p_{i,1} - 1), (p_{i,2} - 1), \dots, (p_{i,k} - 1))},$$

said first station including

means for encoding a digital message word signal M_1 to be transmitted from said first station ($i=1$) to said second station ($i=2$),

means for transforming said digital message word signal $[M_1] M_1$ to one or more message block word signals $[M_1'] M_1''$, each block word signal $[M_1'] M_1''$ being a number representative of a portion of said message word signal M_1 in the range

$$0 \leq M_1'' \leq n_2 - 1, \text{ and}$$

means for transforming each of said message block word signals M_1'' to a ciphertext word signal C_1 using a relationship of the form

12. (Amended) — The communications system of claim 11 further comprising:

$$C_1 \equiv M_1''^{e_2} \pmod{n_2}; \text{ and}$$

means for transmitting said ciphertext word signals C_1 from said first station to said second station, wherein said second station includes

means for deciphering said ciphertext word signals C_1 using $p_{2,1}, p_{2,2}, \dots, p_{2,k}$ to produce said message word signal M_1 .

12. (Twice Amended) The communications system of claim 11, wherein the deciphering means includes

means for decoding said ciphertext word signals C_1 to said message block word signals M_1'' using a relationship of the form

$$M_1'' \equiv C_1^{d_2} \pmod{n_2}, \text{ and}$$

means for transforming said message block word signals M_1'' to said message word signal M_1 .

13. (Twice Amended) A system for communications system of a message cryptographically processed with RSA public key encryption, comprising:

a first station; and

a second station communicatively connected to the first station ~~for communications therebetween,~~

~~the first communicating station having~~

the first station having

encoding means for transforming a transmit message word signal M to a ciphertext word signal C where the transmit message word signal M corresponds to a number representative of a message and

$$0 \leq M \leq n-1$$

n being a composite number formed as a product of at least 3 ~~whole number factors greater than one, the~~ at least 3 factors being distinct random prime numbers, and

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \dots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}, \dots, a_0 are numbers; and

means for transmitting the ciphertext word signal C to the second station, wherein the second station includes means for deciphering the ciphertext word signal C using the at least 3 factors to produce the message.

New Claims:

14. (New Amended) A method of ~~processing~~ communicating a message for use in cryptographic communications cryptographically processed with an RSA public key encryption, comprising the steps of:

selecting a public key portion e associated with a recipient intended for receiving the message;

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

computing a composite number, n , as a product of the k distinct random prime numbers; and;

receiving a ciphertext message formed by encoding a plaintext message data M to a ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, where M represents the message, where $0 \leq M \leq n-1$ and where the sender knows n and the public key portion e but has no access to the k distinct random prime numbers, p_1, p_2, \dots, p_k ; and

deciphering at the recipient the received ciphertext message data C to produce the message, the recipient having access to the k distinct random prime numbers, p_1, p_2, \dots, p_k .

15. (NewAmended) The method according to claim 14, comprising the further step of:
 establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1}(\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))),$$

wherein the deciphering step includes decoding the ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d (\text{mod } n)$.

16. (NewAmended) A method of ~~processing~~communicating a message for use in cryptographic communicationscryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e ;

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1 - 1, p_2 - 1, \dots, p_k - 1$, is relatively prime to the public key portion e ;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1}(\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)));$$

computing a composite number, n , as a product of the k distinct random prime numbers;

~~obtaining~~receiving a ciphertext message data C ; ~~and decoding the ciphertext message data C to~~
representing an encoded form of a plaintext message data M ; and

decoding the received ciphertext message data C to the plaintext message data M using a
relationship of the form $M \equiv C^d (\text{mod } n)$; the decoding performed by a recipient owning
the private key portion d and having access to the k distinct random prime numbers, $p_1,$
 p_2, \dots, p_k .

17. (NewAmended) The method according to claim 16, ~~comprising the further step of:~~
wherein the ciphertext message data C is formed by encoding the plaintext message data M to the
ciphertext message data C ; using a relationship of the form $C \equiv M^e \pmod{n}$, wherewherein $0 \leq M$
 $\leq n-1$ and wherein n and the public key portion e are accessible to the sender although it has no
access to the k distinct random prime numbers, p_1, p_2, \dots, p_k .

18. (NewAmended) A method of ~~processing~~communicating a message ~~for use in~~
~~cryptographic communications~~cryptographically processed with RSA public key encryption,
comprising the steps of:

selecting a public key portion e ;

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each
of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime
to the public key portion e ;

establishing a private key portion d by a relationship to the public key portion e of the form

$$d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))};$$

computing a composite number, n , as a product of the k distinct random prime numbers;

encoding a plaintext message data M with the private key portion d to produce a signed message
 M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$.

receiving the signed message M_s ; and

deciphering the signed message to produce the plaintext message data M .

19. (NewAmended) The method of claim 18 ~~further comprising~~18, wherein the deciphering
step ofincludes:

decoding the signed message M_s with the public key portion e to produce the plaintext message
data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

20. (NewAmended) A method for increasing the efficiency of communicating a cryptographic process message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e ;

developing k

sending to a recipient a cryptographically processed message formed by

assigning a number M to represent the message in plaintext message form, and

cryptographically transforming the assigned number M from the plaintext message form

to a number C that represents the message in an encoded form, wherein the

number C is a function of

the assigned number M ,

a number n that is a composite number equaling the product of at least three

distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking

that each of the k wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of

the at least three distinct random prime numbers minus 1, p_1-1, p_2-1, \dots

p_k-1 , is relatively prime to the public key portion e ;

computing a composite number, n , as a product of the k distinct random prime numbers; and,

wherein the number n and exponent e having been obtained by the sender are associated

with the recipient to which the message is intended; and

receiving the cryptographically processed message which is decipherable by the recipient based

on

the number n ,

another exponent d , and

the number C ,

wherein the exponent d is a function of the exponent e and the at least three distinct

random prime numbers.

21. (Amended) The method according to claim 20,

~~encoding a plaintext message data M to a ciphertext message data C , wherein the~~
cryptographically transforming step includes using a relationship of the form $C \equiv M^e$
 $(\text{mod } n)$, where $0 \leq M \leq n-1$,

~~whereby a computational speed of the cryptographic process is increased.~~

21. (New) — The method according to claim 20, comprising the further step of:

~~establishing a private key portion d by a relationship to the public key portion e in the form of~~
~~;~~ and

~~decoding the ciphertext message data C to the plaintext message data M wherein the exponent d~~
is established based on the at least three distinct random prime numbers, p_1, p_2, \dots, p_k ,
using a relationship of the form $d \equiv e^{-1} (\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$, and

wherein the cryptographically processed message is deciphered using a relationship of the form
 $M \equiv C^d (\text{mod } n)$.

22. (New) Amended A method for ~~increasing the efficiency of~~ communicating a cryptographic
process ~~message cryptographically processed with RSA public key encryption~~, comprising the
steps of:

~~selecting a public key portion e ;~~

~~developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each~~
~~of~~

receiving from a sender a cryptographically processed message, in the form of a number C ,
which is decipherable by the k distinct random prime numbers minus 1, $p_1 - 1, p_2 - 1, \dots, p_k -$
1, is relatively prime to the public key portion e ;

~~establishing a private key portion d by a relationship to the public key portion e in the form of~~

~~;~~

~~computing recipient based on a composite number~~ number n , n , as a product of the k distinct random prime numbers;

~~obtaining a ciphertext message data C ; and an exponent d , and the number C ; and~~

~~decoding the ciphertext~~ deciphering the cryptographically processed message data C to a

wherein a number M represents a plaintext form of the message data M , wherein the

number C represents a cryptographically encoded form of the message and is a function of

the number M ,

the number n that is a composite number equaling the product of at least three

distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of

the at least three distinct random prime numbers,

wherein the number n and exponent e are associated with the recipient to which

the message is intended, and

wherein the exponent d is a function of the exponent e and the at least three

distinct random prime numbers.

23. (Amended) The method according to claim 22,

wherein the number C is formed using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent d is established based on the at least three distinct random prime numbers,

p_1, p_2, \dots, p_k using a relationship of the form $d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))}$,

and wherein the number M is obtained using a relationship of the form $M \equiv C^d \pmod{n}$,

whereby a computational speed of the cryptographic process is increased.

23. (New) — The method according to claim 22, comprising the further step of:

encoding the plaintext message data M to the ciphertext message data C , using a relationship of

the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

24. (New) Amended The method according to claim ~~20,21~~,
wherein p and q are a pair of prime numbers the product of which equals n , and
wherein the deciphering the number C to derive the number M is divided into subtasks, one
subtask for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q ,
whereby for a given length of n it takes fewer computational cycles to ~~find and check the K~~
~~distinct random prime numbers that it takes to find and check~~perform the deciphering
relative to the number of computational cycles for performing such deciphering if the pair
of prime numbers p and q were used instead.

25. (New) Amended The method according to claim 22,
wherein p and q are a pair of prime numbers the product of which equals n , and
wherein the deciphering the number C to derive the number M is divided into subtasks, one
subtask for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q ,
whereby for a given length of n it takes fewer computational cycles to ~~find and check the K~~
~~distinct random prime numbers that it takes to find and check~~perform the deciphering relative to
the number of computational cycles for performing such deciphering if the pair of prime
numbers p and q were used instead.

26. (New) Amended The method according to claim ~~24,20~~,
wherein ~~the~~ p and q are a pair of prime numbers the product of which equals n , and
wherein developing the at least three distinct random prime numbers and computing steps can
ben is performed, including for n that is more than 600 digits long-faster, in less time than
heretofore possible with only it takes to develop the pair of prime numbers p and q and compute
that n .

27. (New) Amended The method according to claim ~~25,22~~,
wherein ~~the~~ p and q are a pair of prime numbers the product of which equals n , and

wherein developing, the at least three distinct random prime numbers and computing and encoding steps can be performed, including for n that is more than 600 digits long faster, in less time than heretofore possible with only it takes to develop the pair of prime numbers p and q and compute that n .

28. (New) Amended) The method according to claim 14,

wherein p and q are a pair of prime numbers the product of which equals n , and

wherein the deciphering step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q ,

whereby for a given length of n it takes fewer computational cycles to ~~find and check the K distinct random prime numbers that it takes to find and check~~ perform the deciphering step relative to the number of computational cycles for performing such deciphering step if the pair of prime numbers p and q were used instead.

29. (New) Amended) The method according to claim 28, 14,

wherein ~~the~~ p and q are a pair of prime numbers the product of which equals n , and

wherein developing the k distinct random prime numbers and computing steps can be the composite number n are performed, including for n that is more than 600 digits long faster, in less time than heretofore possible with only it takes to develop the pair of prime numbers p and q and compute that n .

30. (New) Amended) The method according to claim 16,

wherein p and q are a pair of prime numbers the product of which equals n , and

wherein the decoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q ,

whereby for a given length of n it takes fewer computational cycles to ~~find and check the K distinct random prime numbers that it takes to find and check~~ perform the decoding step relative

to the number of computational cycles for performing such decoding step if the pair of prime numbers p and q were used instead.

31. (New)-Amended) The method according to claim 30,16,

wherein ~~the~~ p and q are a pair of prime numbers the product of which equals n , and

wherein developing the k distinct random prime numbers and computing steps can be the composite n is performed, including for n that is more than 600 digits long-faster, in less time than heretofore possible with only it takes to develop the pair of prime numbers p and q and compute that n .

32. (New)-Amended) The method according to claim 18,

wherein p and q are a pair of prime numbers the product of which equals n ,and

wherein the encoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q ,

whereby for a given length of n it takes fewer computational cycles to ~~find and check the K distinct random prime numbers that it takes to find and check~~perform the encoding step relative to the number of computational cycles for performing such encoding step if the pair of prime numbers p and q were used instead.

33. (New)-Amended) The method according to claim 32,18,

wherein ~~the~~ p and q are a pair of prime numbers the product of which equals n , and

wherein developing the k distinct random prime numbers and computing steps can be the composite number n is performed, including for n that is more than 600 digits long-faster, in less time than heretofore possible with only it takes to develop the pair of prime numbers p and q and compute that n .

34. (New)Amended) The method according to claim 14, wherein a message cryptographically processed in accordance with by the method is compatible sender with two-prime RSA public key cryptography encryption characterized by n being equal to a composite number computed as the

product of 2 prime numbers p and q , is decipherable with multi-prime ($k > 2$) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, \dots, p_k .

35. (NewAmended) The method according to claim 14,9, wherein at the signed message word signal M_{1s} , formed from the digital message word signal M_1 being cryptographically processed in accordance at the first terminal with the method multi-prime ($k > 2$) RSA public key encryption which is compatible characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, \dots, p_k , is decipherable at the second terminal with two-prime RSA public key cryptography encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q .

36. (NewAmended) The method according to claim 16, wherein a message cryptographically processed in accordance with by the method is compatible sender with two-prime RSA public key cryptography encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q , is decipherable by the decoding with multi-prime ($k > 2$) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, \dots, p_k .

37. (NewAmended) The method according to claim 18, wherein at the signed message M_{1s} , formed from the plaintext message data M being cryptographically processed in accordance at the sender with the method multi-prime ($k > 2$) RSA public key encryption which is compatible characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, \dots, p_k , is decipherable by the decoding at the recipient with two-prime RSA public key cryptography encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q .

38. (NewAmended) The method according to claim 20, wherein a message data cryptographically processed in accordance with by the method is compatible sender with two-prime RSA public key cryptography encryption characterized by n being equal to a composite

number computed as the product of 2 prime numbers p and q , is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

39. (NewAmended) The method according to claim 22, wherein a message data cryptographically processed in accordance with by the method is compatible sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q , is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

40. (NewAmended) A cryptography method for local storage of data by a private key owner, comprising the steps of:

selecting a public key portion e ;

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1}(\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)));$$

computing a composite number, n , as a product of the k distinct random prime numbers that are factors of n , where only the private key owner knows the factors of n ; and

encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$, whereby the ciphertext data C is decipherable only by the private key owner having available to it the factors of n .

41. (New) The cryptography method in accordance with claim 40, further comprising the step of:

decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d \pmod{n}$.

42. (NewAmended) A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to ~~conduct encrypted communications~~ communicate with the plurality of stations via the communications medium sending a receiving messages cryptographically processed with an RSA public key encryption, the host system including

at least one cryptosystem ~~responsive to encryption and/or decryption requests from the host system~~, the cryptosystem being configured for

developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to a public key portion e that is associated with the host system,

computing a composite number, n , as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e

in the form of $d \equiv e^{-1}(\text{mod}((p_1-1) \cdot (p_2-1) \cdots (p_k-1)))$,

in response to an encoding request from the host system, encoding a plaintext

message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form $C \equiv M^e (\text{mod } n)$, where $0 \leq M \leq n-1$,

~~establishing a private key portion d by a relationship to the public key portion e~~

~~in the form of~~; and

in response to a decoding request from the host system, decoding a ciphertext message data C communicated via the host producing therefrom a plaintext message data M using a relationship of the form $M \equiv C^d (\text{mod } n)$, where C and M can be respectively C and M .

43. (NewAmended) A system for ~~processing a message used in cryptographic communications~~ of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem ~~operatively~~communicatively coupled to and receiving from the bus encryption~~encoding~~ and decryption~~decoding~~ requests, the cryptosystem being ~~capable~~configured ~~offor~~ providing a public key portion e ,
 developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$,
 checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ,
 computing a composite number, n , as a product of the k distinct random prime numbers,
~~encoding a plaintext form of a first message M to produce a ciphertext form of the first message C using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,~~
 establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} \pmod{((p_1-1) \cdot (p_2-1) \cdots (p_k-1))}$,
in response to an encoding request from the bus, encoding a plaintext form of a first message M to produce C , a ciphertext form of the first message, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$, and
in response to an decoding request from the host system, decoding C' , a ciphertext form of a second message C' , to produce the M' , a plaintext form of the second message M' , using a relationship of the form $M' \equiv C'^d \pmod{n}$, the first and second messages ~~can be being~~ distinct or one and the same.

44. (New) The system of claim 42, wherein the at least one cryptosystem includes a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

45. (New Amended) The system of claim 42, wherein the at least one cryptosystem includes a processor,
 a data-address bus,
 a memory ~~operatively~~ coupled to the processor via the data-address bus,
 a data encryption standard (DES) unit ~~operatively~~ coupled the memory and the processor via the data-address bus,

a plurality of exponentiator elements ~~operatively~~ coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. (New Amended) The system of claim 45, wherein the memory and each of the plurality of exponentiator elements has its own DES unit that ~~encrypts~~ cryptographically processes message data received/returned from/to the processor.

47. (New Amended) The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor, including secure, insecure and exponentiator elements address spaces, and wherein the DES unit ~~that is coupled to the processor~~ is configured to recognize the secure and exponentiator elements address spaces and to automatically ~~encrypt~~ encode message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when the processor is accessing the insecure memory address spaces, the DES unit being further configured to ~~decrypt~~ decode ~~encrypted~~ encoded message data received from the memory before it is provided to the processor.

48. (New) The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

49. (New) The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors p_1, p_2, \dots, p_k .

50. (New Amended) A system for ~~processing a message used in cryptographic communications~~ of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus ~~encryption~~ encoding and ~~decryption~~ decoding requests, the cryptosystem including a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the ~~encryption~~encoding and ~~decryption~~decoding requests, each

~~encryption~~encoding request providing a plaintext message M to be

~~encrypted~~encoded, each ~~encryption~~ request can additionally provide

obtaining a public key that includes an exponent e and a modulus n , a

representation of the modulus n existing in the memory in the form of its

k distinct random prime number factors p_1, p_2, \dots, p_k , where $k \geq 3$, ~~or the~~

~~processor can obtain the public key from the memory,~~

constructing subtasks, one subtask for each of the k factors, to be executed by the

exponentiator elements for producing respective ones of the subtask

values, C_1, C_2, \dots, C_k , and

forming a ciphertext message C from the subtask values C_1, C_2, \dots, C_k ,

wherein the ciphertext message C is decipherable using a private key that includes

the modulus n and an exponent d which is a function of e .

51. (NewAmended) The system of claim 50 wherein each one of the subtasks C_1, C_2, \dots, C_k is developed using a relationship of the form $C_i \equiv M_i^{e_i} \pmod{p_i}$, where $M_i \equiv M \pmod{p_i}$, and $e_i \equiv e \pmod{p_i - 1}$, and where $i=1, 2, \dots, k$.

52. (NewAmended) A system for ~~processing a message used in cryptographic~~ communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus ~~encryption~~encoding and ~~decryption~~decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the ~~encryption~~encoding and ~~decryption~~decoding requests, each ~~encryption/decryption~~encoding/decoding request ~~providing~~provided with a plaintext/ciphertext message M/C to be ~~encrypted/decrypted~~encoded/decoded and ~~can additionally provide with or without~~ a public/private key that includes an exponent e/d and a modulus n ~~a representation of a modulus n which exists in the memory~~ in the form of its k distinct random prime number factors p_1, p_2, \dots, p_k , where $k \geq 3$, ~~or the processor can obtain~~

obtaining the public/private key from the memory, the memory if the encoding/decoding request is provided without the public/private key,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $M_1, M_2, \dots, M_k, C_1, C_2, \dots, C_k$, and forming the ciphertext/plaintext message C/M from the subtask values $C_1, C_2, \dots, C_k/M_1, M_2, \dots, M_k$.

53. (New Amended) The system of claim 52 wherein when produced each one of the subtasks C_1, C_2, \dots, C_k is developed using a relationship of the form $C_i \equiv M_i^{e_i} \pmod{p_i}$, where $C_i \equiv C \pmod{p_i}$, and $e_i \equiv e \pmod{p_i - 1}$, and where $i=1, 2, \dots, k$.

54. (New Amended) The system of claim 52 wherein when produced each one of the subtasks M_1, M_2, \dots, M_k is developed using a relationship of the form $M_i \equiv C_i^{d_i} \pmod{p_i}$, where $M_i \equiv M \pmod{p_i}$, and $d_i \equiv d \pmod{p_i - 1}$, and where $i=1, 2, \dots, k$.

55. (New) —The system of claim 54, wherein the private key exponent d relates to the public key exponent e via $d \equiv e^{-1} \pmod{((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))}$.

56. (New Amended) A system for ~~processing a message used in cryptographic communications~~ of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e ;

means for developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

means for establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$;

means for computing a composite number, n , as a product of the k distinct random prime numbers;

means for ~~obtaining~~receiving a ciphertext message data C ; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d (\text{mod } n)$.

57. (New) The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C , using a relationship of the form $C \equiv M^e (\text{mod } n)$, where $0 \leq M \leq n-1$.

58. (New (Amended)) A system for ~~processing a message used in cryptographic communications of a message cryptographically processed with RSA public key encryption,~~ comprising:

means for selecting a public key portion e ;

means for developing k distinct random prime numbers, p_1, p_2, \dots, p_k , where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \dots, p_k-1$, is relatively prime to the public key portion e ;

means for establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1}(\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$;

means for computing a composite number, n , as a product of the k distinct random prime numbers; and

means for encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$, the signed message M_s being decipherable using the public key portion e .

59. (New Amended) The system of claim 58 further comprising the step of:
means for decoding the signed message M_s with the ~~private~~public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

60. (New Amended) The system of claim 57, wherein the system can ~~conduct encrypted communications with other public key cryptography~~communicate the cryptographically processed message to another system that encrypt/encodes/decrypt/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

61. (New Amended) The system of claim 59, wherein the system can ~~conduct encrypted communications~~communicate the cryptographically processed message to another system that encodes/decodes data with other RSA public key cryptography systems that encrypt/decrypt dataencryption using a modulus value equal to n independent of the k distinct prime numbers.

Document comparison done by DeltaView on Monday, August 26, 2002 08:45:01

Input:	
Document 1	pcdocs://siliconvalley/266556/1
Document 2	pcdocs://siliconvalley/266555/1
Rendering set	Standard

Legend:	
Insertion	
Deletion	
Moved from	
Moved to	
Format change	
Moved deletion	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	407
Deletions	326
Moved from	4
Moved to	4
Format changed	0
Total changes	741

EXHIBIT C

**CONSENT OF ASSIGNEE TO REISSUE
APPLICATION**

Docket Number: 20206-014(PT-TA-410)

This is part of the application for a reissue patent based on the original patent identified below.

Name of
Patentee(s):

COLLINS et al.

Patent Number:

5,848,159

Patent Issued

December 8, 1998

Title of Invention

PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD

As an authorized agent empowered to act on behalf of Compaq Computer Corporation, the assignee of the entire interest in the original patent, I hereby consent to the filing of the present application for reissue of the original patent.



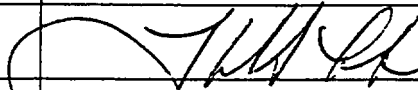
A certificate under 37 CFR(b) is attached.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application, any patent issued thereon, or any patent to which this declaration is directed.

Name of Assignee

Compaq Computer Corporation

Signature of Person
Signing for Assignee



Printed name and title of
person signing for assignee

Theodore S. Park, Counsel

IN THE UNITED STATES PATENTS AND TRADEMARK OFFICE

Applicant: COLLINS et al.

Attorney Docket No.: 20206-0014(PT-TA-410)

Patent No.: 5,848,159

Issued: December 8, 1998

For: "PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"

CERTIFICATE UNDER 37 CFR 3.73(b)

I. Compaq Computer Corporation, a Delaware corporation, certifies that it is the assignee of the entire right, title, and interest in the patent application identified above by virtue of a chain of title from the inventors of the patent application identified above, to the current assignee as shown below:

1. From: Thomas Collins, Dale Hopkins, Susan Langford and Michael Sabin
To: Tandem Computers Incorporated

The document was recorded in the Patent and Trademark Office on May 7, 1997 as Reel and Frame # 8542/0875.

2. From: Tandem Computers Incorporated
To: Compaq Computer Corporation

The document was recorded in the Patent and Trademark Office on October 12, 2000, a copy of which is attached.

The undersigned is empowered to sign this certificate on behalf of the assignee.

Date: 17 OCT 00



Theodore S. Park
Senior Counsel, Intellectual Property

Compaq Computer Corporation
P.O. Box 692000
Houston, TX 7707-2698



3577-04040065
UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

JULY 15, 1997

97 JUL 22 AM 9:59

RECORDED PTAS
TOWNSEND AND TOWNSEND AND CREW LLP
ROBERT J. BENNETT
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CA 94111-3834



100436861A

UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, NORTH TOWER BUILDING, SUITE 10C35, WASHINGTON, D.C. 20231.

RECORDATION DATE: 05/07/1997

REEL/FRAME: 8542/0875
NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

ASSIGNOR:

COLLINS, THOMAS

DOC DATE: 04/29/1997

ASSIGNOR:

HOPKINS, DALE

DOC DATE: 04/29/1997

ASSIGNOR:

LANGFORD, SUSAN

DOC DATE: 04/30/1997

ASSIGNOR:

SABIN, MICHAEL

DOC DATE: 04/30/1997

ASSIGNEE:

TANDEM COMPUTERS INCORPORATED
10435 NORTH TANTAU AVENUE
CUPERTINO, CALIFORNIA 95014

SERIAL NUMBER: 08784453
PATENT NUMBER:

FILING DATE: 01/16/1997
ISSUE DATE:



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

ASSISTANT SECRETARY AND COMMISSIONER
OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

DECEMBER 28, 2000

PTAS

OPPENHEIMER WOLFF & DONNELLY LLP

LEAH SHERRY

1400 PAGE MILL RD.

PALO ALTO, CA 94304



101502720A

**UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT**

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, CG-4, 1213 JEFFERSON DAVIS HWY, SUITE 320, WASHINGTON, D.C. 20231.

RECORDATION DATE: 10/16/2000

REEL/FRAME: 011190/0457
NUMBER OF PAGES: 4

BRIEF: ARTICLES OF MERGER OF PATENT AND SUBSIDIARY CORPORATIONS

ASSIGNOR:

TANDEM COMPUTERS INCORPORATED

DOC DATE: 12/31/1998

ASSIGNEE:

COMPAQ COMPUTER CORPORATION
P.O. BOX 692000, 20555 SH 249
HOUSTON, TEXAS 77070-2698

SERIAL NUMBER: 08784453

PATENT NUMBER: 5848159

FILING DATE: 01/16/1997

ISSUE DATE: 12/08/1998

MARY BENTON, EXAMINER
ASSIGNMENT DIVISION
OFFICE OF PUBLIC RECORDS

RECEIVED
OPPENHEIMER WOLFF & DONNELLY LLP
PALO ALTO, CALIFORNIA

JAN 05 2001

DOC. # 20206-0014
CAL'D _____
FILED ☐ O/M ☐ LS/dt

UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Collins et al.

Patent No. 5,848,159

Issued: December 8, 1998

By: LSB/jmp

Docket No. 20206-014(PT-TA-410) Express No. EL655031318US

For: **PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND
METHOD**

The stamp of the U.S. Patent and Trademark Office hereon acknowledges receipt of the following:

1. Reissue Transmittal along with Fee Transmittal;
2. Petition to Wave Delay Period (37 CFR 1.183);
3. Specification and Claims for U.S. Patent No. 5,484,159;
4. Reissue Declaration by Inventors;
5. Offer to Surrender;
6. Certificate under 37 CFR 3.73(b);
7. Consent of Assignee to Reissue Patent;
8. Copy of Assignments;
9. Preliminary Amendment;
10. IDS Transmittal, 1449, and 13 cited references; and
11. Check No. 124516 for \$2,664..00.

JC914 U.S. PTO

09/694416



10/20/00

[illegible]

Form 1449 (Modified) Information Disclosure Statement By Applicant (Use Several Sheets if Necessary)	Docket No. 20206.126	Reexamination No.: 90/005,773
	Applicant:	90/005,773
	Filing Date 12-8-98	Group



U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
JWS	A	4,351,982	9-28-82	Miller et al.	178	22.10; 22.11	12-15-80
JWS	B	5,974,151	10-26-99	Slavin	380	30	11-1-96
	C						
	D						
	E						
	F						
	G						
	H						
	I						
	J						
	K						

RECEIVED
JUN 8 2001

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	L							
	M							
	N							
	O							
	P							

Technology Center 2600

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	R	
	S	
	T	

RECEIVED

JUL 02 2001

Technology Center 2100

Examiner <i>James Seal</i>	Date Considered <i>14 June 2002</i>
-------------------------------	--

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE, PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE STATEMENT BY APPLICANT	REISSUE APPLICATION NO. 09/694,416 REEXAMINATION CONTROL NO. 90/005/733 REEXAMINATION CONTROL NO. 90/005/733 Orig. PATENT NO. 5,848,159	ATTY DOCKET NO.: 20206-125 (PT-TA410) 20206-126 (PT-TA410US-4) 20206-127 (PT-TA410US-5) respectively.
	INVENTORS COLLINS et al.	
	ISSUE DATE December 8, 1998	GROUP

U. S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
JWS	AA	4,514,592	4/30/1985	Miyaguchi	178	22.11; 22.14	7/14/1982
JWS	AB	5,046,094	9/3/1991	Kawamura	380	46; 28	2/2/1990
JWS	AC	5,343,527	8/30/1994	Moore	380	4; 25; 30	10/27/1993

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	NAME	CLASS	SUBCLASS	TRANSLATION YES
	AD							

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

JWS	AE	P. J. Flinn et al. Using the RSA Algorithm for Encryption and Digital Signatures: Can you Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?" July 9, 1997, Alston & Bird LLP, http://www.cyberlaw.com/rsa.html
-----	----	--

EXAMINER <i>James Seal</i>	DATE CONSIDERED 5 Dec 2001
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE STATEMENT BY APPLICANT	ATTY DOCKET NO 20206-0014(PT-TA-410)	PATENT NO. 5,848,159
	APPLICANT COLLINS et al.	
	ISSUE DATE December 8, 1998	GROUP 2766

U. S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA	5,761,310	06/1998	Naciri	380	30	07/18/1996

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	NAME	CLASS	SUBCLASS
	AB						

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

JWS	AC	S.A. VANSTONE et al., "Using Four-Prime RSA in Which Some of the Bits are Specified," December 1994, Electronics Letter, Vol. 30, No. 25. pp. 2118-2119.
JWS	AD	C. Couvruer et al., "An Introduction to Fast Generation of Large Prime Numbers," 1982, Philips Journal Research, Vol. 37, Nos. 5-6, pp. 231-264.
JWS	AE	Y. DESMEDT et al., "Public-Key Systems Based on the Difficulty of Tampering (Is There a Difference Between DES and RSA?)," 1986, Lecture Notes in Computer Science, Advances in Cryptology-CRYPTO '86. Proceedings.
JWS	AF	J. J. QUISQUATER et al., "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem" October 1982, Electronic Letters, Vol. 19, No. 21.
JWS	AG	CETIN KAYA KOC, "High-Speed RSA Implementation (Version 2.0)," November 1994, RSA White Paper, RSA Laboratories.
JWS	AH	RIVEST et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," February 1978, Communications of the ACM, Vol. 21.
JWS	AI	PKCS #1: RSA Encryption Standard (Version 1.5), November 1993, RSA Laboratories Technical Note.
JWS	AJ	M.O. RABIN, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization," January, 1979, MIT Laboratory for Computer Science.
JWS	AK	R. LIDL et al., "Permutation Polynomials in RSA-Cryptosystems," 1984, Advances in Cryptology—Crypto '83, pp. 293-301.
JWS	AL	D. BONEH et al., "Generating a Product of Three Primes with an Unknown Factorization," Computer Science Department, Stanford University.
JWS	AM	J. J. QUISQUATER et al., "Fast Generation of Large Prime Numbers" June 1982, Library of Congress, Catalog No. 72-179437, IEEE Catalog No. 82CH1767-3 IT, pp. 114-115
JWS	AN	A. J. Menezes et al., "Handbook of Applied Cryptography", 1997, Library of Congress catalog No. 96-27609, pp. 89, 612-613

EXAMINER <i>James Seal</i>	DATE CONSIDERED <i>5 Dec 2001</i>
EXAMINER. Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant	